

Урок 3 Видео 2

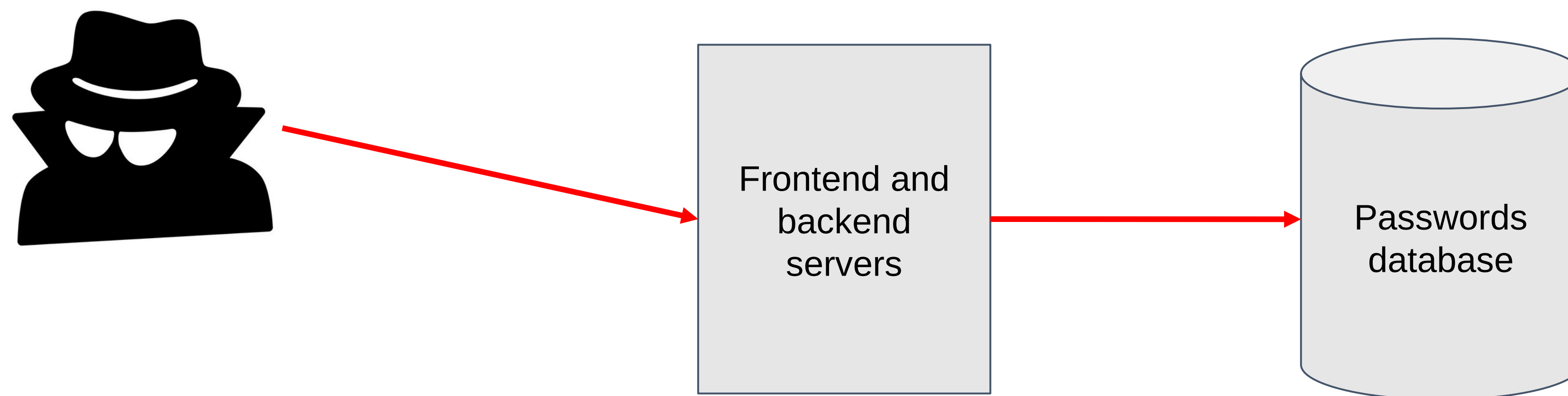
Криптография

Dictionary Attack on hashes

В этом видео

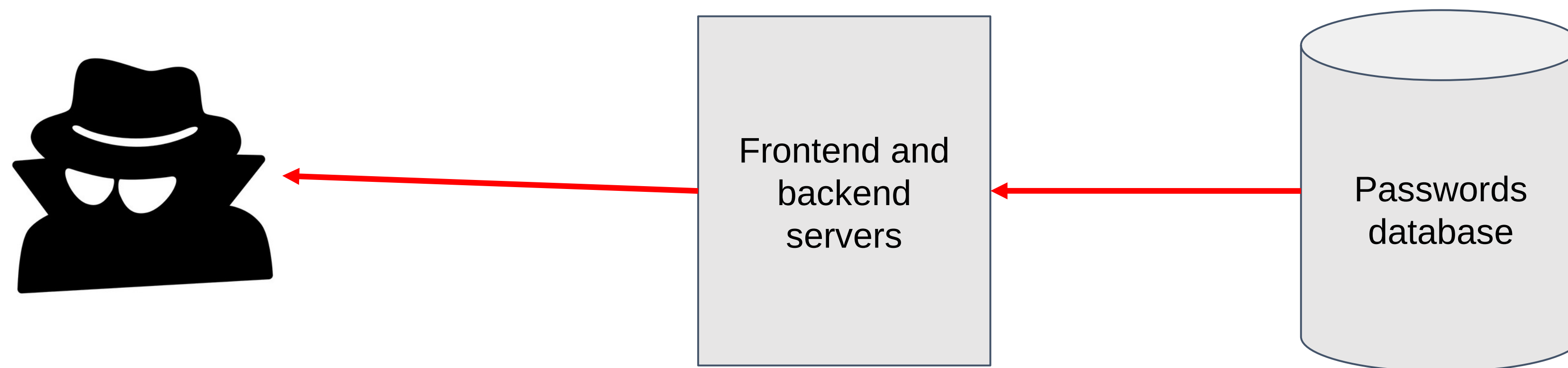
1. Недостатки схемы хранения хешированных паролей
2. hashcat
3. “Соленые” хеши

Хранение хешей от паролей



f447b20a7fcbf53a5d5be013ea0b15af
d577273ff885c3f84dadb8578bb41399
b2cfa4183267af678ea06c7407d4d6d8
...

Хранение хешей от паролей



f447b20a7fcbf53a5d5be013ea0b15af
d577273ff885c3f84dadb8578bb41399
b2cfa4183267af678ea06c7407d4d6d8
…

Хранение хешей от паролей

123456789 → f447b20a7fcbf53a5d5be013ea0b15af
password → d577273ff885c3f84dadb8578bb41399
iloveyou → b2cfa4183267af678ea06c7407d4d6d8
… → …



8d6d4d7047c60ae876fa7623814afc2b
d577273ff885c3f84dadb8578bb41399
b2cfa4183267af678ea06c7407d4d6d8
…

Space-time trade-off

Можно увеличить скорость алгоритма, кешируя определенные значения в RAM или на диск.



“Соленые” хеши

Соль — это случайная строка, которая добавляется к сообщению, чтобы для двух одинаковых сообщений получился разный хеш.



Итоги

1. Узнали про недостатки схемы хранения хешированных паролей
2. Научились использовать hashcat для перебора хешей
3. Узнали как устроены “соленые” хеши